Title: Advanced Routing Protocol Security

Contact:

Thomas Clausen, thomas.clausen@polytechnique.edu
Network Research Groupe of Ecole Polytechnique

A number of routing protocols (but, not only routing protocols) base their correct functioning on the recipient of a control message "trusting" that the originator of the message, as well as any intermediate systems on the path from the originator to the recipient, have been "doing the right thing": generating a message with semantically correct content, and modifying the message in transit according to protocol rules. The way that "trusting" is implemented is by way of adding cryptographic signatures to an outgoing control message, allowing the recipient to verify that the message has not been modified in transit.
If message sizes and computational resources were not an issue, then simply replicating and stacking messages and standard signatures at each hop would provide nice properties: an "audit trail" of the path the message has taken, as well as authentication of the originator of the message. However, with "common" signature sizes and cryptographic algorithms, this would quickly (after a couple of hops) incur an excessive overhead.
Fortunately, aggregate signature mechanisms exist, allowing (if messages are not modified in transit) each forwarder to not add, but update, the message signature - while preserving the "audit trail" previously described.
Unfortunately, a great number of routing (but not just) protocols requires modification of a message in transit (the trivial case is when a path metric is updated each time a message is forwarded), this system breaks: the originator generated signature becomes invalid after the first hop.

Fortunately, we have an idea of how we -- under certain conditions -- can permit both mutable messages, and aggregate signatures. Testing - and if it works - making real that idea, is what this project is about. Specifically, to:

1. Investigate the use of aggregate signatures, permitting tractable mutable messages.
2. Develop a prototype/demonstrator of (at least) one routing protocol using these aggregate signatures.
3. Investigate appropriate cryptographic primitives (RSA, ECC, ...) and parameters for signature schemes as applied to the routing protocol(s) in the demonstrators. This must take into account factors such as MTUs, power consumption, computational ressources, etc.
4. Develop and document this as a general framework applicable across a large set of routing protocols such as those described above.